REMARKS

Initially, Applicant notes that the remarks and amendments made by this paper are consistent with the proposals presented to the Examiner during the telephone call of January 30, 2008 and which appear to overcome all of the rejections of record for at least the reasons presented over the phone and in this response.

By this response, claims 11 and 20-24 have been amended and no claims have been added or canceled, such that claims 1-2, 5, 8, 11, 14, 19-24, and 27-33 remain pending, of which claims 1, 19, 20, and 27 are the only independent claims at issue.[1]

The Office Action, mailed December 31, 2007, considered and rejected claims 1-2, 5, 8, 11, 14, 19-24, and 27-33 and claim 14 was rejected under 35 U.S.C. § 112, second paragraph for being dependent on a cancelled claim. Claims 1-2, 5, 8, 11, 14, 19-24, and 27-33 were rejected under 35 U.S.C. §112, first paragraph for purportedly failing to comply with the written description requirement. Claims 1-2, 5, 8, 11, 19-24, and 27-33 were rejected under 35 U.S.C. § 102(e) as being anticipated by Prasad et al, (U.S. Patent No. 6,675,152), hereinafter Prasad. Claim 14 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Prasad in view of Peinado (U.S. Patent No 7,073,063), hereinafter Peinado.

It will be noted that dependent claim 14 has been amended to depend upon claim 11 and no longer depends on canceled claim 12. In view of the present amendment to the claim, Applicant respectfully requests that the rejection of claim 14 under 35 U.S.C. §112, second paragraph, be withdrawn.

With regard to the rejection of the claims under 35 U.S.C. §112, first paragraph, Applicant respectfully submits that the claims are fully supported by the specification. While the specification uses the terms server and client when describing the embodiments of the invention, the specification clearly states that such terms are utilized to simplify the explanation and that the trusted entity will be referred to as the server and the untrusted entity will be referred to as the client. Therefore, anywhere in the specification that references a server or a client is merely shorthand for trusted and untrusted entity, respectively. In view of this language, the use of the terms trusted entity and untrusted entity enjoys support to the same degree as the terms server and client.

---

[1] Support for the claim amendments is found throughout the Specification and more particularly on page 14 of the Application as originally filed. Accordingly, Applicant respectfully submits that the claim amendments do not add new manner, and entry thereof is respectfully requested.

With regard to the issue of a temporary signature, on page 15 of the Application as originally filed, the Specification reads "The server receives the data and signature from the client in a step 338 and computes a **temporary signature** in step 340 using the same HMAC...". Since the term "server" is short for "trusted entity", there is support for the trusted entity computing a temporary signature.

As reflected above, the pending claims are currently directed to embodiments for ensuring that data stored by an untrusted entity is not in an altered state when it is subsequently accessed. Claim 1, for example, recites a method for ensuring that data stored in a persistent storage of an untrusted entity by the untrusted entity have not been modified when the data are subsequently accessed for use by the untrusted entity. The method comprises sending data related information to a trusted entity to compute a signature of the data. The trusted entity employs a key that is only known and available for use by a trusted entity to compute a signature for the data related information before the data are stored in the persistent storage by the untrusted entity. The trusted entity then sends the signature to the untrusted entity and the signature and the data are then stored in the persistent storage of the untrusted entity. Before the stored data are subsequently used by the untrusted entity, the unaltered state of the data is verified by sending the data related information back to the trusted entity for verification. The trusted entity utilizes the key that is only known and available for use by the trusted entity to generate a temporary signature based on the stored data that is compared with the stored signature. The stored data are then only used by untrusted entity if the step of verifying indicates that the data that were stored have not been changed since the signature was computed before storing the data.

The remaining independent claims are closely related to claim 1. For example, claim 19 recites a computer program product corresponding to claim 1, while claims 20 and 27 are directed to embodiment for systems performing methods similar to claim 1 from the perspective of an untrusted entity and a trusted entity, respectively. Additionally, the untrusted entity of claim 20 is restricted to a gaming device and the data is specific to game session data that will be used in a subsequent gaming session on the device.

Applicant respectfully submits that the cited art of record, whether considered alone or in combination, fails to render the pending claims unpatentable for at least the reason that Prasad and Peinado fail to teach or suggest each and every element of the current claims. For example,

while Prasad and the current claimed invention each generally relate to data verification, many distinctions are present within the claims that Prasad does not address. As an example, the present claims require that the signature for the data related information be computed using a **key known only to the trusted entity**. Such an element is not present within Prasad. Furthermore, the untrusted entity stores the information and the signature in the present claims, whereas Prasad expressly discloses that the data and signature are stored in a centralized database.

In particular, Prasad is directed to embodiments for ensuring that data stored in a database of a gaming network have not been tampered with. In Prasad, a signature of a transaction is calculated based on transaction related information, and the signature and the transaction information are sent to a central database for storage, or to some other storage location. Upon subsequent access to the data, the transaction signature is verified. Verifying the transaction signature includes verification of the transaction signature stored in the **database** and a signature calculated on the transaction information at the time of access. Additionally, the signature stored in an alternate location may be periodically compared to the signatures stored at the database to detect tampering.

Notably, however, Prasad fails to disclose that the key is known only to the trusted entity, as recited in the pending claims in combination with the other claim elements. Specifically, while Prasad states that any technique for generating the signature may be employed, the only mention of using a cryptographic key is the use of a key to encrypt a previously computed signature. Prasad is silent as to the key being used to compute the signature or what entity has knowledge of the key. Without these elements, Applicant respectfully submits that Prasad, standing on its own, cannot fully anticipate the claimed embodiments.

Additionally, the claimed embodiments require that the signature for the data be stored at the **untrusted entity**, and it is this signature that is compared to the temporary signature. In Prasad, on the other hand, the signature is stored at the central database and it is the signature that is stored at the central database that is used to verify a temporary signature. While the signature at other locations is described in Prasad, the signature is only used in comparison against the centrally stored signature.[2] In view of the fact that Prasad does not teach or suggest a signature stored at the untrusted entity being validated against a temporary signature computed

[2] See column 10, lines 16-40 where the process of validating the database signatures is described.

by the trusted entity, as recited with the other elements of the claims, Applicant respectfully submits that the claims are patentable over the cited art of Prasad.

While only the specific limitations of claim 1 have been discussed, independent claims 19, 20, and 27 were rejected using the same rationale as claim 1 and the above arguments are therefore appropriate for those claims as well. It will be appreciated that because the all of the independent claims have been addressed, each dependent claim is allowable over the cited art for at least the same reasons, and the other rejections and assertions of record with respect to the other dependent claims are now moot, and therefore need not be addressed individually. Nevertheless, to further differentiate between the cited references and the present invention, independent claim 20 and its associated dependent claims will be further addressed.

Independent claim 20 is similar to the previously addressed claims; however, it is specific to a game system embodiment. In particular, the claims recite that the device is a gaming device and that the data is game session data for use by the device in subsequent game sessions. This is in direct contrast with Prasad, which discloses that data is transaction related data and is **not** relevant to a future gaming session. Furthermore, the untrusted entity in Prasad is a terminal that does not actually contain the game and is not properly a gaming device. For these reasons, in addition to the previously mentioned reasons, Applicant respectfully submits that claim 20 and its dependent claims are allowable over the cited art.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and such that any of the remaining rejections and assertions made, particularly with respect to all of the dependent claims, do not need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice, and particularly with regard to the dependent claims.[3]

[3] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting any official notice taken. Furthermore, although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should the need arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 28th day of March, 2008.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
COLBY J. NUTTALL
Registration No.
JOHN C. BACOCH
Registration No. 59,890
Attorneys for Applicant
Customer No. 47973

RDN:CJN:JCB:ahy
MS 810 62 - DRAFT AmendC after non-final (OA dated 31dec2007)VIA eFILE
PATENT APPLICATION